Practitioner's Docket No. 770P009542-US(PCT)

CHAPTER II 10/009206

Preliminary Classification:

Proposed Class:

Subclass:

NOTE: *"All applicants are requested to include a preliminary classification on newly filed patent applications. The preliminary classification, preferably class and subclass designations, should be identified in the upper right-hand corner of the letter of transmittal accompanying the application papers, for example 'Proposed Class 2, subclass 129.'" M.P.E.P., § 601, 7th ed.*

TRANSMITTAL LETTER TO THE UNITED STATES ELECTED OFFICE (EO/US) (ENTRY INTO U.S. NATIONAL PHASE UNDER CHAPTER II)

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/12721	9 May 2000	13 May 1999

TITLE OF INVENTION

TECHNIQUE FOR SECURE REMOTE CONFIGURATION OF A SYSTEM

APPLICANT(S)

George M. BROOKNER

Box PCT
Assistant Commissioner for Patents
Washington D.C. 20231
ATTENTION: EO/US

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

☒ deposited with the United States Postal Service in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

37 C.F.R. § 1.8(a)

☐ with sufficient postage as first class mail.

37 C.F.R. § 1.10 *

☒ as "Express Mail Post Office to Addressee"
Mailing Label No. EL627510644US (mandatory)

TRANSMISSION

☐ facsimile transmitted to the Patent and Trademark Office, (703) _____-_____.

Shauna Murphy
Signature

Date: November 8, 2001

Shauna Murphy
(type or print name of person certifying)

* *Only the date of filing (§ 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under § 1.8 continues to be taken into account in determining timeliness. See § 1.703(f). Consider "Express Mail Post Office to Addressee" (§ 1.10) or facsimile transmission (§ 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

NOTE: To avoid abandonment of the application, the applicant shall furnish to the USPTO, not later than 20 months from the priority date: (1) a copy of the international application, unless it has been previously communicated by the International Bureau or unless it was originally filed in the USPTO; and (2) the basic national fee (see 37 C.F.R. § 1.492(a)). The 30-month time limit may not be extended. 37 C.F.R. § 1.495.

WARNING: *Where the items are those which can be submitted to complete the entry of the international application into the national phase are subsequent to 30 months from the priority date the application is still considered to be in the international state and if mailing procedures are utilized to obtain a date the express mail procedure of 37 C.F.R. § 1.10 must be used (since international application papers are not covered by an ordinary certificate of mailing—See 37 C.F.R. § 1.8.*

NOTE: Documents and fees must be clearly identified as a submission to enter the national state under 35 U.S.C. § 371 otherwise the submission will be considered as being made under 35 U.S.C. § 111. 37 C.F.R. § 1.494(f).

I. Applicant herewith submits to the United States Elected Office (EO/US) the following items under 35 U.S.C. § 371:

a. ☒ This express request to immediately begin national examination procedures (35 U.S.C. § 371(f)).

b. ☒ The U.S. National Fee (35 U.S.C. § 371(c)(1)) and other fees (37 C.F.R. § 1.492) as indicated below:

2. Fees

CLAIMS FEE	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
☐*	TOTAL CLAIMS 35	35 −20=	15	× $18.00=	$ 270.00
	INDEPENDENT CLAIMS 6	6 −3=	3	× $84.00 =	252.00
	MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+$ 280.00 =	
BASIC FEE**	☒ U.S. PTO WAS INTERNATIONAL PRELIMINARY EXAMINATION AUTHORITY Where an international preliminary examination fee as set forth in § 1.482 has been paid on the international application to the U.S. PTO: ☒ and the international preliminary examination report states that the criteria of novelty, inventive step (non-obviousness) and industrial activity, as defined in PCT Article 33(1) to (4) have been satisfied for all the claims presented in the application entering the national stage (37 C.F.R. § 1.492(a)(4)) ..... $100.00 ☐ and the above requirements are not met (37 C.F.R. § 1.492(a)(1)) .....$ 710.00 ☐ U.S. PTO WAS NOT INTERNATIONAL PRELIMINARY EXAMINATION AUTHORITY Where no international preliminary examination fee as set forth in § 1.482 has been paid to the U.S. PTO, and payment of an international search fee as set forth in § 1.445(a)(2) to the U.S. PTO: ☐ has been paid (37 C.F.R. § 1.492(a)(2)) .....$ 740.00 ☐ has not been paid (37 C.F.R. § 1.492(a)(3)) ..$1,040.00 ☐ where a search report on the international application has been prepared by the European Patent Office or the Japanese Patent Office (37 C.F.R. § 1.492(a)(5)) ..... $ 890.00				100.00
	Total of above Calculations				= 622.00
SMALL ENTITY	Reduction by 1/2 for filing by small entity, if applicable. Assertion must be made. (note 37 C.F.R. § 1.27)				–
	Subtotal				
	Total National Fee				$ 622.00
	Fee for recording the enclosed assignment document $40.00 (37 C.F.R. § 1.21(h)). (See Item 13 below). See attached "ASSIGNMENT COVER SHEET".				
TOTAL	Total Fees enclosed				$ 622.00

*See attached Preliminary Amendment Reducing the Number of Claims.

☒ Attached is a ☒ check ☐ money order in the amount of $ 622.00

☐ Authorization is hereby made to charge the amount of $ _____

☒ to Deposit Account No. 16-1350

☐ to Credit card as shown on the attached credit card information authorization form PTO-2038.

WARNING: *Credit card information should* ***not*** *be included on this form as it may become public.*

☒ Charge any additional fees required by this paper or credit any overpayment in the manner authorized above.

A duplicate of this paper is attached.

"WARNING: *"To avoid abandonment of the application the applicant shall furnish to the United States Patent and Trademark Office not later than the expiration of 30 months from the priority date: * * * (2) the basic national fee (see § 1.492(a)). The 30-month time limit may not be extended." 37 C.F.R. § 1.495(b).*

WARNING: *If the translation of the international application and/or the oath or declaration have not been submitted by the applicant within thirty (30) months from the priority date, such requirements may be met within a time period set by the Office. 37 C.F.R. § 1.495(b)(2). The payment of the surcharge set forth in § 1.492(e) is required as a condition for accepting the oath or declaration later than thirty (30) months after the priority date. The payment of the processing fee set forth in § 1.492(f) is required for acceptance of an English translation later than thirty (30) months after the priority date. Failure to comply with these requirements will result in abandonment of the application. The provisions of § 1.136 apply to the period which is set. Notice of Jan. 3, 1993, 1147 O.G. 29 to 40.*

☐ **Assertion of Small Entity Status**

☐ **Applicant hereby asserts status as a small entity under 37 C.F.R. § 1.27.**

NOTE: 37 C.F.R. § 1.27(c) deals with the assertion of small entity status, whether by a written specific declaration thereof or by payment as a small entity of the basic filing fee or the fee for the entry into the national phase as states:

"(c) Assertion of small entity status. Any party (person, small business concern or nonprofit organization) should make a determination, pursuant to paragraph (f) of this section, of entitlement to be accorded small entity status based on the definitions set forth in paragraph (a) of this section, and must, in order to establish small entity status for the purpose of paying small entity fees, actually make an assertion of entitlement to small entity status, in the manner set forth in paragraphs (c)(1) or (c)(3) of this section, in the application or patent in which such small entity fees are to be paid.

(1) Assertion by writing. Small entity status may be established by a written assertion of entitlement to small entity status. A written assertion must:

(i) Be clearly identifiable;

(ii) Be signed (see paragraph (c)(2) of this section); and

(iii) Convey the concept of entitlement to small entity status, such as by stating that applicant is a small entity, or that small entity status is entitled to be asserted for the application or patent. While no specific words or wording are required to assert small entity status, the intent to assert small entity status must be clearly indicated in order to comply with the assertion requirement.

(2) Parties who can sign and file the written assertion. The written assertion can be signed by:

(i) One of the parties identified in §§ 1.33(b) (e.g., an attorney or agent registered with the Office), §§ 3.73(b) of this chapter notwithstanding, who can also file the written assertion;

(ii) At least one of the individuals identified as an inventor (even though a §§ 1.63 executed oath or declaration has not been submitted), notwithstanding §§ 1.33(b)(4), who can also file the written assertion pursuant to the exception under §§ 1.33(b) of this part; or

(iii) An assignee of an undivided part interest, notwithstanding §§ 1.33(b)(3) and 3.73(b) of this chapter, but the partial assignee cannot file the assertion without resort to a party identified under §§ 1.33(b) of this part.

(3) Assertion by payment of the small entity basic filing or basic national fee. The payment, by any party, of the exact amount of one of the small entity basic filing fees set forth in §§ 1.16(a), (f), (g), (h), or (k), or one of the small entity basic national fees set forth in §§ 1.492(a)(1), (a)(2), (a)(3), (a)(4), or (a)(5), will be treated as a written assertion of entitlement to small entity status even if the type of basic filing or basic national fee is inadvertently selected in error.

(i) If the Office accords small entity status based on payment of a small entity basic filing or basic national fee under paragraph (c)(3) of this section that is not applicable to that application, any balance of the small entity fee that is applicable to that application will be due along with the appropriate surcharge set forth in §§ 1.16(e), or §§ 1.16(l).

(ii) The payment of any small entity fee other than those set forth in paragraph (c)(3) of this section (whether in the exact fee amount or not) will not be treated as a written assertion of entitlement to small entity status and will not be sufficient to establish small entity status in an application or a patent."

3. ☒ A copy of the International application as filed (35 U.S.C. § 371(c)(2)):

NOTE: Section 1.495 (b) was amended to require that the basic national fee and a copy of the international application must be filed with the Office by 30 months from the priority date to avoid abandonment. "The International Bureau normally provides the copy of the international application to the Office in accordance with PCT Article 20. At the same time, the International Bureau notifies applicant of the communication to the Office. In accordance with PCT Rule 47.1, that notice shall be accepted by all designated offices as conclusive evidence that the communication has duly taken place. Thus, if the applicant desires to enter the national stage, the applicant normally need only check to be sure the notice from the International Bureau has been received and then pay the basic national fee by 30 months from the priority date." Notice of Jan. 7, 1993, 1147 O.G. 29 to 40, at 35-36. See item 14c below.

a. ☒ is transmitted herewith.

b. ☒ is not required, as the application was filed with the United States Receiving Office.

c. ☒ has been transmitted

i. ☒ by the International Bureau.

Date of mailing of the application (from form PCT/1B/308):

11/23/00.

ii. ☐ by applicant on _____. *(Date)*

4. ☒ A translation of the International application into the English language (35 U.S.C. § 371(c)(2)):

a. ☐ is transmitted herewith.

b. ☒ is not required as the application was filed in English.

c. ☐ was previously transmitted by applicant on _____. *(Date)*

d. ☐ will follow.

5. [X] Amendments to the claims of the International application under PCT Article 19 (35 U.S.C. § 371(c)(3)):

NOTE: *The Notice of January 7, 1993 points out that 37 C.F.R. § 1.495(a) was amended to clarify the existing and continuing practice that PCT Article 19 amendments must be submitted by 30 months from the priority date and this deadline may not be extended. The Notice further advises that: "The failure to do so will not result in loss of the subject matter of the PCT Article 19 amendments. Applicant may submit that subject matter in a preliminary amendment filed under section 1.121. In many cases, filing an amendment under section 1.121 is preferable since grammatical or idiomatic errors may be corrected." 1147 O.G. 29-40, at 36.*

a. ☐ are transmitted herewith.

b. ☐ have been transmitted

i. ☐ by the International Bureau.

Date of mailing of the amendment (from form PCT/1B/308):

_____.

ii. ☐ by applicant on _____. *(Date)*

c. [XX] have not been transmitted as

i. [XX] applicant chose not to make amendments under PCT Article 19. Date of mailing of Search Report (from form PCT/ISA/210.):

8/23/00.

ii. ☐ the time limit for the submission of amendments has not yet expired. The amendments or a statement that amendments have not been made will be transmitted before the expiration of the time limit under PCT Rule 46.1.

6. [X] A translation of the amendments to the claims under PCT Article 19 (38 U.S.C. § 371(c)(3)):

a. ☐ is transmitted herewith.

b. ☐ is not required as the amendments were made in the English language.

c. [XX] has not been transmitted for reasons indicated at point 5(c) above.

7. [X] A copy of the international examination report (PCT/IPEA/409)

[XX] is transmitted herewith.

☐ is not required as the application was filed with the United States Receiving Office.

8. ☐ Annex(es) to the international preliminary examination report

a. ☐ is/are transmitted herewith.

b. ☐ is/are not required as the application was filed with the United States Receiving Office.

9. ☐ A translation of the annexes to the international preliminary examination report

a. ☐ is transmitted herewith.

b. ☐ is not required as the annexes are in the English language.

10. ☒ An oath or declaration of the inventor (35 U.S.C. § 371(c)(4)) complying with 35 U.S.C. § 115

    a. ☐ was previously submitted by applicant on _____. *(Date)*

    b. ☐ is submitted herewith, and such oath or declaration

        i. ☐ is attached to the application.

        ii. ☐ identifies the application and any amendments under PCT Article 19 that were transmitted as stated in points 3(b) or 3(c) and 5(b); and states that they were reviewed by the inventor as required by 37 C.F.R. § 1.70.

    c. ☒ will follow.

II. Other document(s) or information included:

11. ☒☒ An International Search Report (PCT/ISA/210) or Declaration under PCT Article 17(2)(a):

    a. ☒☒ is transmitted herewith.

    b. ☒ has been transmitted by the International Bureau.

        Date of mailing (from form PCT/IB/308): 11/23/00.

    c. ☐ is not required, as the application was searched by the United States International Searching Authority.

    d. ☐ will be transmitted promptly upon request.

    e. ☐ has been submitted by applicant on _____. *(Date)*

12. ☒ An Information Disclosure Statement under 37 C.F.R. §§ 1.97 and 1.98:

    a. ☒ is transmitted herewith.

    Also transmitted herewith is/are:

        ☒ Form PTO-1449 (PTO/SB/08A and 08B).

        ☒☒ Copies of citations listed.

    b. ☐ will be transmitted within THREE MONTHS of the date of submission of requirements under 35 U.S.C. § 371(c).

    c. ☐ was previously submitted by applicant on _____. *(Date)*

13. ☐ An assignment document is transmitted herewith for recording.

    A separate ☐ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.

_____

_____

_____

14. ☒ Additional documents:
   a. ☒ Copy of request (PCT/RO/101)
   b. ☒ International Publication No. WO 00/70503
      i. ☒ Specification, claims and drawing
      ii. ☐ Front page only
   c. ☒ Preliminary amendment (37 C.F.R. § 1.121)
   d. ☒ Other
   PCT/RO/105; PCT/RO/106; PCT/RO/146; PCT/RO/101; PCT/ISA/202; PCT/DO/EO/901(a)
   PCT/RO/102; PCT/IB/301; PCT/ISA/220;PCT/IPEA/401;PCT/IB/304; PCT/IB/306;
   PCT/IPEA/402; PCT/IB/308; PCT/IB/332; PCT/IPEA/416; Written Opinion

15. ☒ The above checked items are being transmitted
   a. ☒ before 30 months from any claimed priority date.
   b. ☐ after 30 months.

16. ☐ Certain requirements under 35 U.S.C. § 371 were previously submitted by the applicant on ____________, namely:

____

____

____

____

____

AUTHORIZATION TO CHARGE ADDITIONAL FEES

WARNING: *Accurately count claims, especially multiple dependant claims, to avoid unexpected high charges if extra claims are authorized.*

NOTE: *"A written request may be submitted in an application that is an authorization to treat any concurrent or future reply, requiring a petition for an extension of time under this paragraph for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. An authorization to charge all required fees, fees under § 1.17, or all required extension of time fees will be treated as a constructive petition for an extension of time in any concurrent or future reply requiring a petition for an extension of time under this paragraph for its timely submission. Submission of the fee set forth in § 1.17(a) will also be treated as a constructive petition for an extension of time in any concurrent reply requiring a petition for an extension of time under this paragraph for its timely submission." 37 C.F.R. § 1.136(a)(3).*

NOTE: *"Amounts of twenty-five dollars or less will not be returned unless specifically requested within a reasonable time, nor will the payer be notified of such amounts; amounts over twenty-five dollars may be returned by check or, if requested, by credit to a deposit account." 37 C.F.R. § 1.26(a).*

☒ Please charge, in the manner authorized above, the following additional fees that may be required by this paper and during the entire pendency of this application:

   ☒ 37 C.F.R. § 1.492(a)(1), (2), (3), and (4) (filing fees)

WARNING: *Because failure to pay the national fee within 30 months without extension (37 C.F.R. § 1.495(b)(2)) results in abandonment of the application, it would be best to always check the above box.*

☒ 37 C.F.R. § 1.492(b), (c) and (d) (presentation of extra claims).

NOTE: Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 C.F.R. § 1.492(d)), it might be best not to authorize the PTO to charge additional claim fees, except possible when dealing with amendments after final action.

☒ 37 C.F.R. § 1.17 (application processing fees)

☒ 37 C.F.R. § 1.17(a)(1)–(5) (extension fees pursuant to § 1.136(a).

☐ 37 C.F.R. § 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b))

NOTE: Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 C.F.R. § 1.311(b).

NOTE: 37 C.F.R. § 1.28(b) requires "Notification of any change in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying . . . issue fee." From the wording of 37 C.F.R. § 1.28(b): (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.

☒ 37 C.F.R. § 1.492(e) and (f) (surcharge fees for filing the declaration and/or filing an English translation of an International Application later than 30 months after the priority date).

SIGNATURE OF PRACTITIONER

Clarence A. Green

(type or print name of practitioner)

PERMAN & GREEN, LLP

P.O. Address

425 Post Road, Fairfield, CT 06430 USA

Reg. No.: 24,622

Tel. No.: (203) 259-1800

Customer No.: 2512

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Express Mail No.: EL627510644US
Applicant(s): George M. BROOKNER
INTERNATIONAL APPLICATION NO.: PCT/US00/12721
INTERNATIONAL FILING DATE: 5/9/00
TITLE: TECHNIQUE FOR SECURE REMOTE CONFIGURATION OF A SYSTEM
ATTORNEY DOCKET NO.: 770P009542-US(PCT)

Box PCT
Commissioner of Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Dear Sir:

Please amend the above-identified, patent application as follows:

IN THE SPECIFICATION:

After the Title and before the first paragraph, please insert the following paragraph:

This application claims the benefit of the earlier filed International Application No. PCT/US00/12721, International Filing Date, May 9, 2000, which designated the United States of America, and which international application was published under PCT Article 21(2) in English as WO Publication No. WO 00/70503.

Respectfully submitted,

Clarence A. Green Reg. No.: 24,622
PERMAN & GREEN, LLP
425 Post Road, Fairfield, CT 06430
(203)259-1800
Customer No.: 2512

8 Nov 01
Date

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

EXPRESS MAIL NO.: EL627432156US

APPLICANT: George M. Brookner

INTERNATIONAL APPLICATION NO.: PCT/US00/12721

INTERNATIONAL FILING DATE: 5/9/00

US SERIAL NUMBER: 10/009,206 EXAMINER:

TITLE: TECHNIQUE FOR SECURE REMOTE CONFIGURATION OF A SYSTEM

ATTORNEY DOCKET NO.: 770P009542-US(PCT)

Commissioner of Patents
BOX PCT
Washington, D.C. 20231

TRANSMITTAL OF COMBINED DECLARATION AND POWER OF ATTORNEY DOCUMENT

Dear Sir:

We are submitting herewith the executed Combined Declaration and Power of Attorney document for the above-referenced patent application. It is noted that we have not yet received the Notification of Missing Requirements. Enclosed is a check for $130.00 (surcharge for late filing of Combined Declaration and Power of Attorney). Please charge any additional fees due to our deposit account no. 16-1350.

Respectfully submitted,

6 March 02

Clarence A. Green, Reg. No. 24,622 Date
PERMAN & GREEN, LLP
425 Post Road
Fairfield, CT 06430
(203) 259-1800 Customer No. 2515

Description

TECHNIQUE FOR SECURE REMOTE CONFIGURATION OF A SYSTEM

Technical Field

The invention relates to a technique for system configuration, and more particularly to a technique for remotely configuring a system through a communications network in a secure manner.

Background of the Invention

Use of processor-controlled (P-C) products, e.g., personal and hand-held computers, wireless information devices, postage franking systems, etc. is ubiquitous. However, people may utilize these P-C products differently to satisfy their individual needs. For that reason, P-C product manufacturers offer different options to customers for them to individualize the products. Typically, when a customer orders a P-C product from a manufacturer, he/she specifies the desired options for the product. In response, the manufacturer starts with a basic pre-assembled system having a generic configuration, and adds the specified options thereto to customize the system. The manufacturer then ships the resulting system to the customer to fulfill the order.

Summary of the Invention

The customization by manufacturers of P-C products described above is beneficial to a customer in that the customer pays only for the product having the configuration specified by him/her, without overspending on some product features which the customer does not need. However, I have identified certain aspects of the prior art practice as being particularly disadvantageous. For example, after selecting a P-C product, a customer needs to wait for the manufacturer customization, which may take a long time because of a backlog. It is

particularly frustrating for a customer after he/she spends much time selecting the desired P-C product in a store and cannot immediately bring home the product because of the need of the manufacturer customization.

I have recognized that in the manufacturer customization, the bulk of the time is expended on installing the software options specified by the customer in a basic system having a generic configuration. I have also recognized that most of the P-C products have a modem device therein or provide for similar capabilities for communicating data over a communications network. Thus, in accordance with the invention, the customer may be provided with the basic pre-assembled system having modem capabilities, and on his/her own download the specified software components onto the system from a server to customize the system. Advantageously, by shifting the customization burden onto the customer in accordance with the invention, the customer can be in possession of a P-C product as soon as the purchase thereof is consummated. In addition, the product manufacturer saves on the otherwise labor and time for installing the software options for the customer.

In accordance with the invention, a server is employed for configuring P-C devices through a communications network. Records associated with the devices are stored in the server. On initial power up of one such P-C device, the P-C device automatically generates a request for configuration thereof to the server through the communications network. This request includes coded information resulting from encrypting at least an identifier, e.g., a serial number, identifying the P-C device, or alternatively from cryptographically signing at least part of the request. In response to such a request, the server locates a record associated with the P-C device, and verifies the identity of the P-C device based on the coded information. The record includes second information concerning a device

configuration specified by the customer. Only when the identity of the P-C device is verified, does the server provide through the communications network to the P-C device information objects, e.g., software components and/or data, for realization of the specified configuration based on the second information.

Brief Description of the Drawing

Further objects, features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying drawing, in which:

Fig. 1 illustrates an arrangement for configuring a system in accordance with the invention;

Fig. 2 illustrates the format of a system record stored in a server in the arrangement of Fig. 1; and

Fig. 3 illustrates a routine for providing software components from the server to the system to realize a specified system configuration.

Detailed Description

Fig. 1 illustrates an arrangement embodying the principles of the invention in which a processor-controlled (P-C) system may be customized through a communications network. By way of example, this system is illustratively a franking system, numerically denoted 105, for generating postage indicia which serve as proof of payment of postage.

In accordance with the invention, system 105 when delivered to a user has a generic configuration, which includes processing unit 107 comprising one or more conventional processors, non-volatile memory 109, static random access memory (SRAM) 111, communications facility 113 which includes a modem device or similar circuitry or network card, and necessary hardware components 115 for carrying out the generation of postage indicia. This

generic configuration allows subsequent system customization by the user to satisfy his/her individual needs. For example, in accordance with the invention, the user later may on his/her own integrate specified software options into system 105 to customize same. Thus, the manufacturer of system 105 in this instance does not customize the system for the user as in prior art. As a result, system 105 advantageously can be delivered to the user soon after the user places the order thereof. At the same time, the manufacturer saves on the otherwise labor and time for customizing system 105 for the user.

Server 130, which may be administered and maintained by the manufacturer of system 105, provides through communications network 145 the specified software options to realize the user customization in accordance with the invention. Communications network 145 may be, e.g., the Internet, a telephone network or other public or private network. Server 130 includes processor 133, memory 135, and interface 141 for establishing a communication connection with the systems served thereby, e.g., system 105. When the user orders system 105 with certain software and hardware options selected by the user, the manufacturer causes system 105 having a generic configuration and the selected hardware options delivered to the user. At the same time, the manufacturer causes server 130 to create a record therein, registering the selected software options and/or hardware options of system 105. Without loss of generality, in this instance the software options but not the hardware options are registered in such a record. To that end, database 137 is maintained by server 130 in memory 135, which contains system records 139-1 through 139-N, associated with N different systems served by server 130, respectively, where N represents an integer greater than zero. Without loss of generality, let's assume here that system record 139-1 is associated with system 105.

Fig. 2 illustrates the format of a generic system record denoted 200. As shown in Fig. 2, record 200 includes field 203 containing a system public key for decrypting messages from the system associated with the record in a manner described below, field 205 containing a serial number assigned to the system for identifying same, and field 207 contains identifiers indicating the software options selected by the user.

When the user receives the package containing system 105 having the generic configuration, and selected hardware components for realizing the hardware options specified by the user, the user connects the selected hardware components to system 105 pursuant to the instructions provided by the manufacturer. To realize the software options specified by the user, programs such as booter 121 including basic input/output system (BIOS) functions, and loader 123 are provided and pre-stored in non-volatile memory 109 in system 105. On initial power up of system 105 and connection thereof to network 145 through communication facility 113, booter 121 is invoked which performs conventional system start-up functions which include, among others, causing loader 123 to be copied into SRAM 111 at a specified location to which a program vector points. Directed by the program vector, processing unit 107 executes the code of loader 123 in SRAM 111.

Instructed by the code of loader 123, unit 107 causes communications facility 113 to establish a communication connection with server 130 through network 145. Unit 107 transmits a configuration request for software components from server 130 to realize the specified software options. However, in accordance with an aspect of the invention, security measures are implemented to ensure that system 105 is a legitimate system to receive the software components from server 130. For example, a cryptographic methodology may be implemented to encrypt and/or cryptographically sign

certain information in the request from system 105. The success by server 130 in decrypting the resulting encrypted information and/or authenticating the resulting digital signature verifies the identity and legitimacy of system 105. One such cryptographic methodology is the RSA methodology, named after its developers, Rivest, Shamir and Adleman. For details on the RSA methodology, one may refer to: R. Rivest et al., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, February 1978. The RSA methodology involves a public key algorithm which uses a private key and a public key for data encryption. Unlike a private key which is securely protected from the public, a public key can be published and made known to the public. The keys for the RSA algorithm are generated mathematically, and are computational inverses to each other. The success of the RSA methodology depends on the use of very large numbers for the keys.

Thus, for example, in implementing the RSA methodology here, a key pair consisting of system public key 125 and system private key 127 are assigned to system 105, which are pre-stored in memory 109. In addition, as mentioned before a serial number, denoted 129, is assigned to system 105 to identify same, which is pre-stored in memory 109. In this instance, the aforementioned configuration request by system 105 includes information concerning (a) system public key 125 and (b) serial number 129 which is encrypted using system private key 127 in accordance with the RSA methodology.

Upon receiving the configuration request through interface 141, as indicated at step 302 in Fig. 3, processor 133 at step 305 searches database 137 for any system record having field 203 thereof matching system public key 125 in the request. If no such record is found, processor 133 at step 308 denies the configuration request. Otherwise, if any such record

(e.g., record 139-1 associated with system 105 in this instance) is found, processor 133 at step 311 decrypts the encrypted serial number in the request using received system public key 125 or alternatively the matching system public key in field 203 of the record, in accordance with the RSA methodology. Processor 133 at step 314 determines whether the resulting serial number matches that in field 205 of the record. If they do not match, processor 133 at step 317 denies the configuration request. Otherwise, if they match, processor 133 at step 320 reads from field 207 of the record the identifiers indicating the software options specified by the user for installation in system 105. Based on such identifiers, processor 133 at step 323 retrieves from software component storage 143 those software components for realizing the specified software options. To ensure secure transmission, and prevent unauthorized use, of such software components to system 105, processor 133 at step 326 encrypts the software components using server private key 145, in accordance with the RSA methodology. Processor 133 at step 329 transmits the encrypted software components to system 105 through the established communication connection.

After receiving the encrypted software components, processing unit 107 in system 105 utilizes server public key 152, which corresponds to server private key 145 and is pre-stored in memory 109, to decrypt the received software components. The resulting software components, which contain software identifications (IDs) in their headers, are then loaded into SRAM 111, in accordance with a program vector table. This program vector table, e.g., in the form of a memory map, specifies the memory locations in SRAM 111 for the respective software components identified by their software IDs, and thus the order of execution of these software components. As processing unit 107 executes the downloaded software components, the specified software

options are realized.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise numerous other arrangements which embody the principles of the invention and are thus within its spirit and scope.

For example, the invention is disclosed in the context of an initial configuration of system 105 after it is delivered to the user. However, it is apparent from the disclosure heretofore that the inventive methodology is equally applicable to a re-configuration of the system after the initial configuration. In that case, loader 123 can be re-invoked to download additional software components from server 130 to modify the initial configuration.

Moreover, in the disclosed embodiment, software components are downloaded to system 105 from server 130 to realize desired system options. It is apparent that selected data, e.g., those concerning the user and/or his/her preferences, may also be downloaded to the system to customize same.

In addition, in the disclosed embodiment, server 130 maintains system record 200 for each system served thereby. The information in field 207 of record 200 enables server 130 to keep track of the current configuration of the system. Server 130 may also rely on the software IDs of the downloaded software components to keep track of the current configuration of the system. Such software IDs may contain version numbers of the respective downloaded software components and may also form part of record 200. When any new versions of the downloaded software components become available, with the knowledge of the current version number of each downloaded software component in the system, server 130 can effectively inform the user of such new versions for upgrading purposes. Moreover, the software IDs identifying the downloaded software components currently

installed in the system may also be cataloged and stored in the system itself. In that case, a re-configuration of the system can be accomplished in a more secure manner by downloading additional software components together with an authorization code from server 130. As described in PCT International Publication No. WO 99/66422, published on December 23, 1999, such an authorization code may be derived by server 130 from, among others, the serial number of the system and new software IDs identifying the additional software components. After receiving the additional software components including the software IDs in their headers, and the authorization code, the system independently generates an authorization code based on the received software IDs and the serial number stored in the system. Only if the generated authorization code corresponds to the received authorization code, is the system allowed to install the additional software components therein.

Further, in the disclosed embodiment, the configuration request by system 105 includes information, e.g., the serial number identifying system 105, which is encrypted. However, as mentioned before, such information may be cryptographically signed using the RSA or other cryptographic methodology such as the digital signature algorithm (DSA) or Elliptic Curve algorithm, instead. In that case, the authentication of the resulting digital signature verifies the identity of system 105.

Finally, server 130 and system 105 are disclosed herein in a form in which various functions are performed by discrete functional blocks. However, any one or more of these functions could equally well be embodied in an arrangement in which the functions of any one or more of those blocks or indeed, all of the functions thereof, are realized, for example, by one or more appropriate memories, and/or appropriately programmed processors.

Claims

1. Apparatus for serving a plurality of devices through a communications network, the apparatus comprising:

a memory for storing a plurality of records associated with the devices, respectively;

an input element for receiving from a selected device a request for configuration thereof through the communications network, the request including coded information;

a processor responsive to the request for locating a record associated with the selected device, and verifying an identity of the selected device based on the coded information, the record including second information concerning a selected configuration; and

an output element for providing through the communications network to the selected device information objects for realization of the selected configuration based on the second information when the identity of the selected device is verified.

2. The apparatus of claim 1 wherein the coded information including encrypted information concerning the identity of the selected device.

3. The apparatus of claim 2 wherein the encrypted information concerns a serial number of the selected device.

4. The apparatus of claim 2 wherein the encrypted information is encrypted in accordance with a public key algorithm.

5. The apparatus of claim 1 wherein the coded information including a digital signature resulting from cryptographically signing at least part of the request.

6. The apparatus of claim 1 wherein the information objects include software components.

7. The apparatus of claim 1 wherein the information objects include data.

8. Apparatus configurable by a server through a communications network, the apparatus comprising:

storage for storing a cryptographic element;

a processor for generating a request which includes therein coded information for verification by the server of an identity of the apparatus, the coded information being generated using the cryptographic element;

an interface for receiving information objects for configuring the apparatus from the server through the communications network when the identity of the apparatus is verified by the server;

a memory; and

a loader for directing the information objects to be loaded in the memory in accordance with a predetermined plan.

9. The apparatus of claim 8 wherein the cryptographic element includes a private key.

10. The apparatus of claim 8 wherein the request is automatically generated on an initial power up of the apparatus.

11. The apparatus of claim 8 wherein the coded information including a digital signature resulting from cryptographically signing at least part of the request.

12. The apparatus of claim 8 comprising a franking system.

13. The apparatus of claim 8 wherein the

information objects include software components.

14. The apparatus of claim 8 wherein the information objects include data.

15. Apparatus for serving a plurality of devices through a communications network, the apparatus comprising:

a memory for storing a plurality of records associated with the devices, respectively;

an input element for receiving from a selected device a request for configuration thereof through the communications network, the request including a cryptographic element, and first information concerning a first identifier identifying the selected device, the first information being encrypted;

a processor for selecting a record based on the cryptographic element, the selected record including a second identifier and configuration information, the processor determining whether the second identifier corresponds to the first identifier obtained by decrypting the first information using the cryptographic element; and

an output element for causing the selected device to be configured based on the configuration information when it is determined that the second identifier corresponds to the first identifier.

16. The apparatus of claim 15 wherein the cryptographic element includes a public key.

17. The apparatus of claim 15 wherein the first identifier includes a serial number of the selected device.

18. The apparatus of claim 15 wherein the first information is encrypted in accordance with a public key

algorithm.

19. A method for use in an apparatus for serving a plurality of devices through a communications network, the method comprising:

storing a plurality of records associated with the devices, respectively;

receiving from a selected device a request for configuration thereof through the communications network, the request including coded information;

in response to the request, locating a record associated with the selected device;

verifying an identity of the selected device based on the coded information, the record including second information concerning a selected configuration; and

providing through the communications network to the selected device information objects for realization of the selected configuration based on the second information when the identity of the selected device is verified.

20. The method of claim 19 wherein the coded information including encrypted information concerning the identity of the selected device.

21. The method of claim 20 wherein the encrypted information concerns a serial number of the selected device.

22. The method of claim 20 wherein the encrypted information is encrypted in accordance with a public key algorithm.

23. The method of claim 19 wherein the coded information including a digital signature resulting from cryptographically signing at least part of the request.

24. The method of claim 19 wherein the information objects include software components.

25. The method of claim 19 wherein the information objects include data.

26. A method for use in an apparatus configurable by a server through a communications network, the apparatus including a memory, the method comprising:

storing a cryptographic element;

generating a request which includes therein coded information for verification by the server of an identity of the apparatus, the coded information being generated using the cryptographic element;

receiving information objects for configuring the apparatus from the server through the communications network when the identity of the apparatus is verified by the server; and

loading the information objects in the memory in accordance with a predetermined plan.

27. The method of claim 26 wherein the cryptographic element includes a private key.

28. The method of claim 26 wherein the request is automatically generated on an initial power up of the apparatus.

29. The method of claim 26 wherein the coded information including a digital signature resulting from cryptographically signing at least part of the request.

30. The method of claim 26 wherein the information objects include software components.

31. The method of claim 26 wherein the information objects include data.

32. A method for use in an apparatus for serving a plurality of devices through a communications network, the method comprising:

storing a plurality of records associated with the devices, respectively;

receiving from a selected device a request for configuration thereof through the communications network, the request including a cryptographic element, and first information concerning a first identifier identifying the selected device, the first information being encrypted;

selecting a record based on the cryptographic element, the selected record including a second identifier and configuration information;

determining whether the second identifier corresponds to the first identifier obtained by decrypting the first information using the cryptographic element; and

causing the selected device to be configured based on the configuration information when it is determined that the second identifier corresponds to the first identifier.

33. The method of claim 32 wherein the cryptographic element includes a public key.

34. The method of claim 32 wherein the first identifier includes a serial number of the selected device.

35. The method of claim 32 wherein the first information is encrypted in accordance with a public key algorithm.

FIG. 1

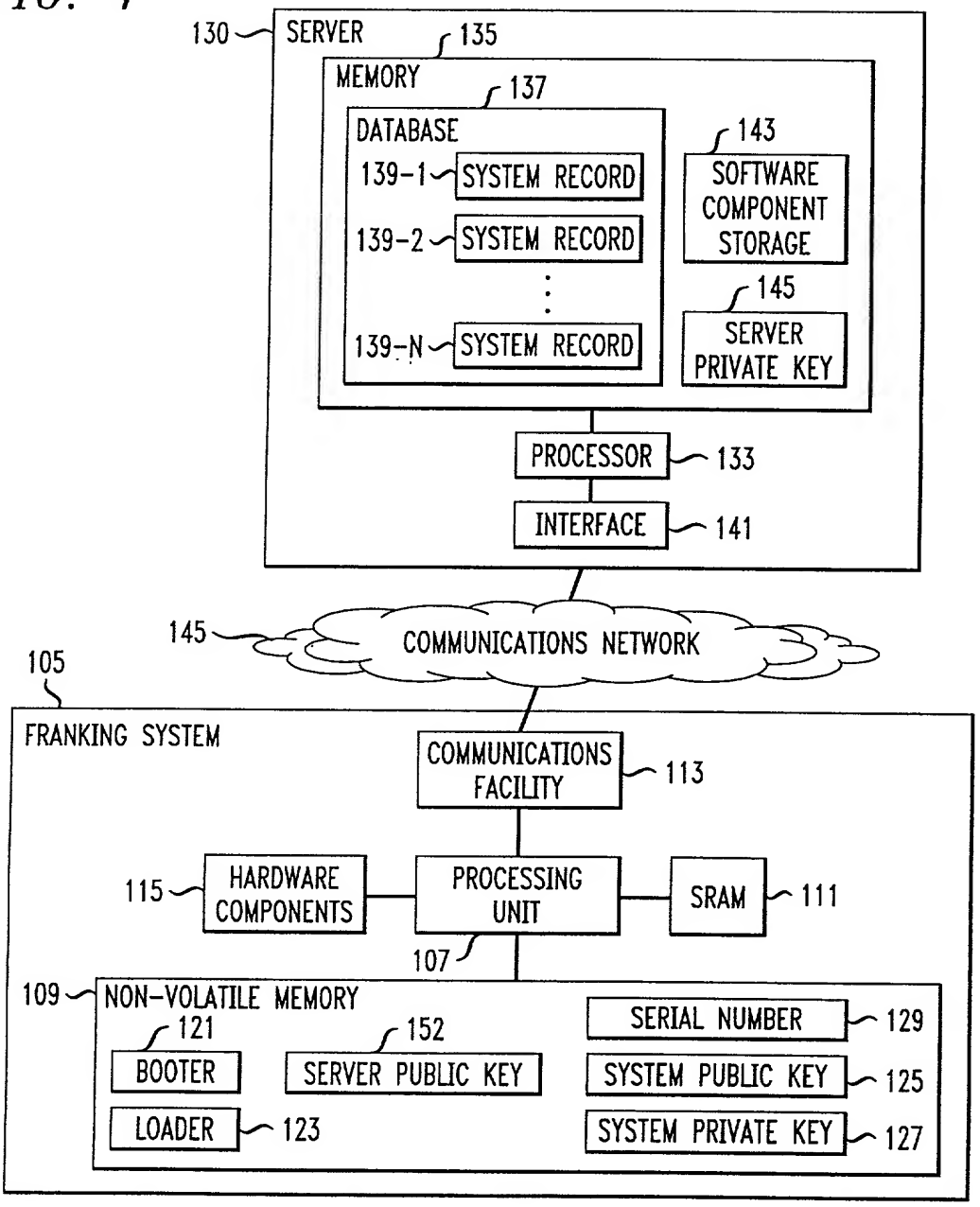

130
SERVER
135
MEMORY
137
DATABASE
139-1
SYSTEM RECORD
139-2
SYSTEM RECORD
139-N
SYSTEM RECORD
143
SOFTWARE COMPONENT STORAGE
145
SERVER PRIVATE KEY
PROCESSOR
133
INTERFACE
141
145
COMMUNICATIONS NETWORK
105
FRANKING SYSTEM
COMMUNICATIONS FACILITY
113
115
HARDWARE COMPONENTS
PROCESSING UNIT
SRAM
111
107
109
NON-VOLATILE MEMORY
121
BOOTER
152
SERVER PUBLIC KEY
LOADER
123
SERIAL NUMBER
129
SYSTEM PUBLIC KEY
125
SYSTEM PRIVATE KEY
127

FIG. 2

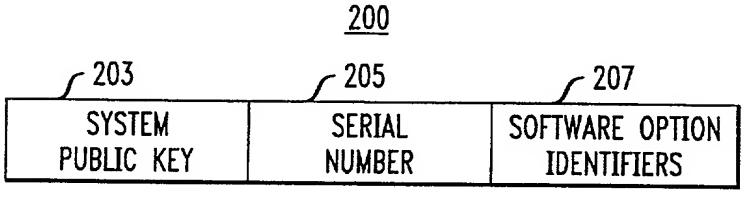
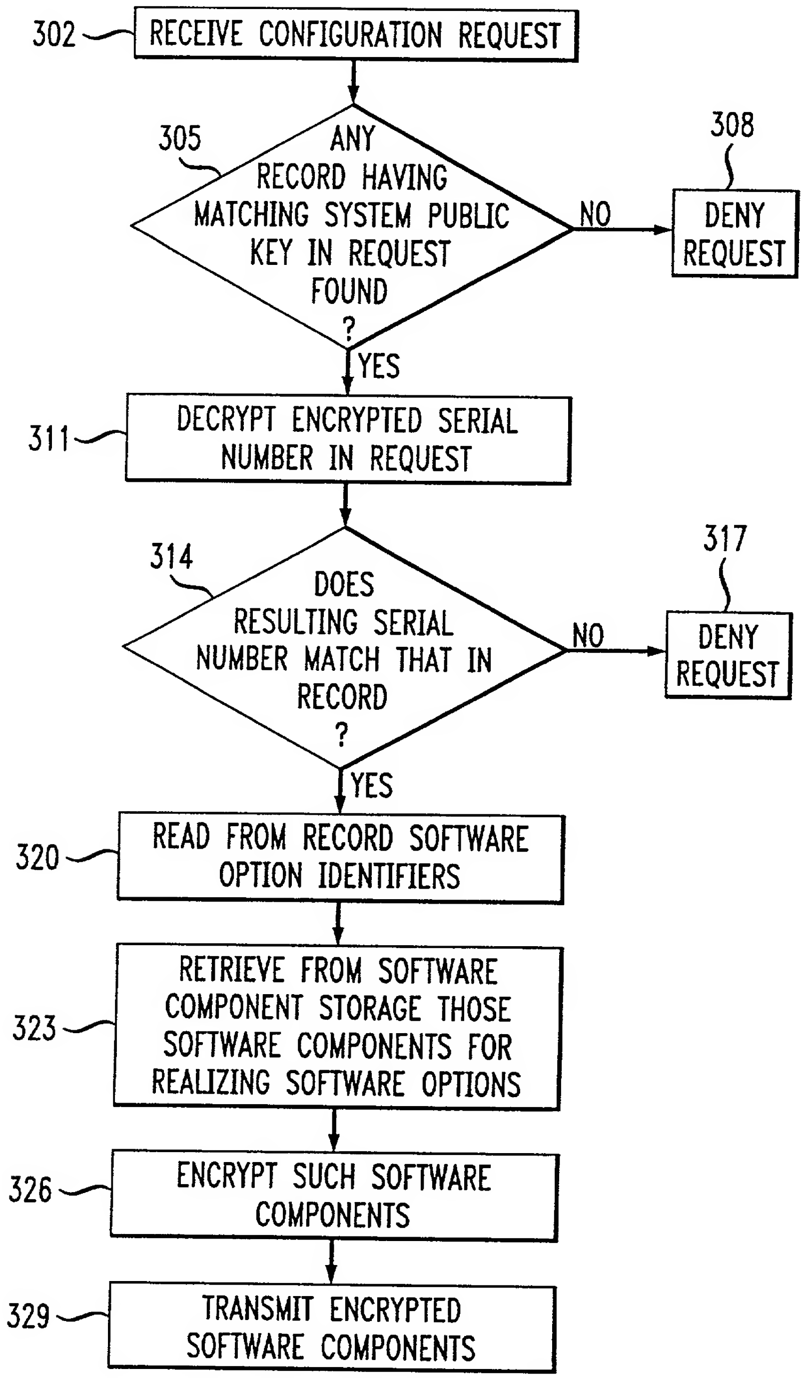

200
203
205
207
SYSTEM PUBLIC KEY
SERIAL NUMBER
SOFTWARE OPTION IDENTIFIERS

FIG. 3



Docket No.: 770P009542-US(PCT)

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Title: TECHNIQUE FOR SECURE REMOTE CONFIGURATION OF A SYSTEM

the specification of which

(check one)

☐ is attached hereto.

X was filed on as United States Application No.10/009,206

or PCT International Application Number PCT/US00/12721 filed on May 9, 2000

and was amended on (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International Application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed

Prior Foreign Application(s)

(Number)	(Country)	(Day/Month/Year Filed)	Priority Not Claimed
PCT/US00/12721	PCT	9 May 2000	☐
			☐
			☐
			☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

60/133,921 (Application Serial No.) — May 13, 1999 (Filing Date)

_____ (Application Serial No.) — (Filing Date)

_____ (Application Serial No.: — (Filing Date)

I hereby claim the benefit under 35 U.S.C. Section 120 of any United States application(s), or Section 365(c) of any PCT International Application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International Application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C.F.R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

_____ (Application Serial No.) _____ (Filing Date) (Status) (patented, pending, abandoned)

_____ (Application Serial No.) (Filing Date) (Status) (patented, pending, abandoned)

_____ (Application Serial No.) _____ (Filing Date) (Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

All attorneys listed under Customer No.: 2512

Send Correspondence to:

Customer No.: 2512

Direct Telephone Calls to: (name and telephone number)
Clarence A. Green, Reg. No.: 24,622 (203) 259-1800

Full name of sole or first inventor. George M. BROOKNER
Sole or first inventor's signature. DATE Jan. 4, 2004
Residence: 11 Surrey Drive, Norwalk , Connecticut 06851 CT
Citizenship USA
Post Office Address 11 Surrey Drive, Norwalk , Connecticut 06851

Full name of second inventor:
Second inventor's signature: DATE
Residence address:
Citizenship
Post Office Address